2161
#5
04-9-2

Docket No. 217573US2/btm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Noriaki OGISHIMA

GAU: 2161

SERIAL NO: 10/022,773

EXAMINER:

FILED: December 20, 2001

FOR: IMAGE FORMING APPARATUS, ENCIPHERED DATA PROCESSING METHOD AND ENCIPHERED DATA PROCESSING SYSTEM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-391242	December 22, 2000
JAPAN	2001-380452	December 13, 2001

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

10/022,773

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２０００年１２月２２日

出 願 番 号
Application Number: 特願２０００－３９１２４２

出 願 人
Applicant(s): 株式会社リコー

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年１２月１４日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　0003799
【提出日】　平成12年12月22日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　3/12
【発明の名称】　暗号化印刷システム
【請求項の数】　10
【発明者】
【住所又は居所】　東京都大田区中馬込１丁目３番６号
株式会社リコー内
【氏名】　荻島　則明
【特許出願人】
【識別番号】　000006747
【氏名又は名称】　株式会社リコー
【代表者】　桜井　正光
【手数料の表示】
【予納台帳番号】　003724
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

出証特２００１－３１０８４８２

【書類名】　明細書

【発明の名称】　暗号化印刷システム

【特許請求の範囲】

【請求項１】　ネットワークを利用して、デジタルコンテンツのデータを配信する配信手段と、

前記データを暗号化する暗号化手段と、を有する配信端末と、

前記配信端末から前記データの配信を要求するユーザ端末と、

前記ユーザ端末に接続され、前記暗号化手段により暗号化されたデータを復号化する復号化手段を有する印刷装置と、を有し、

前記配信端末は、前記ユーザ端末に要求された前記データを前記暗号化手段により暗号化して前記ユーザ端末に送信し、

前記ユーザ端末は、前記配信端末より受信したデータを前記印刷装置に送信し、

前記印刷装置は、前記ユーザ端末より受信したデータを前記復号化手段により復号化して印刷することを特徴とする暗号化印刷システム。

【請求項２】　前記配信端末は、

ユーザに対し前記データの配信についての課金処理を行う課金処理手段をさらに有することを特徴とする請求項１記載の暗号化印刷システム。

【請求項３】　前記印刷装置は、

前記暗号化手段および前記復号化手段により使用される、前記印刷装置固有の、所定のデータ列から成る暗号鍵と、

該暗号鍵を管理し、前記ユーザ端末から該暗号鍵の取得要求があった際、該暗号鍵を前記ユーザ端末へ送信する暗号鍵管理手段と、をさらに有し、

前記ユーザ端末は、あらかじめ、あるいは、前記配信端末より要求があった場合、前記印刷装置の前記暗号鍵管理手段より前記暗号鍵を取得して、前記配信端末へ送信し、

前記配信端末は、前記ユーザ端末を介して取得した前記暗号鍵を用いて、前記暗号化手段により、前記ユーザ端末から要求された前記データを暗号化し、

前記印刷装置は、前記ユーザ端末より受信した前記暗号化手段により暗号化さ

れたデータを、前記暗号鍵を用いて、前記復号化手段により復号化することを特徴とする請求項１または２記載の暗号化印刷システム。

【請求項４】　前記ネットワークは、インターネットであり、

前記印刷装置は、

ＩＰアドレスをさらに有し、

前記暗号鍵は該ＩＰアドレスであることを特徴とする請求項３記載の暗号化印刷システム。

【請求項５】　前記暗号鍵は、

装置製造番号であることを特徴とする請求項３記載の暗号化印刷システム。

【請求項６】　前記印刷装置は、

ランダム変数を生成するランダム変数生成手段をさらに有し、

前記暗号鍵管理手段は、

前記ユーザ端末による前記暗号鍵の取得要求があった場合、前記ランダム変数生成手段によりランダム変数を生成し、前記暗号鍵に、該ランダム変数を組み合わせて、ランダム暗号鍵を作成し、該ランダム暗号鍵を保管および前記ユーザ端末へ送信し、

前記暗号化手段および前記復号化手段は、前記ランダム暗号鍵を使用して前記データの暗号化および復号化を行うことを特徴とする請求項３から５のいずれか１項に記載の暗号化印刷システム。

【請求項７】　前記ランダム変数生成手段は、

前記ランダム変数として、現在時刻を利用することを特徴とする請求項６記載の暗号化印刷システム。

【請求項８】　前記ランダム変数生成手段は、

前記ランダム変数として、Ｔｏｔａｌカウンタの値を利用することを特徴とする請求項６記載の暗号化印刷システム。

【請求項９】　前記印刷装置は、デジタル複写機能を有する複合機であることを特徴とする請求項１から８のいずれか１項に記載の暗号化印刷システム。

【請求項１０】　前記印刷装置は、ファクシミリ機能を有する複合機であることを特徴とする請求項１から８のいずれか１項に記載の暗号化印刷システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルコンテンツ配信の際の配信データの複製防止を企図する暗号化印刷システムに関する。

【０００２】

【従来の技術】

従来から、ネットワーク上において、文字情報、画像データ、音声データなど各種のデジタルデータを有料もしくは無料で配信するサービスが盛んに行われている。デジタルデータは、容易に複製が可能であり、データを有料で配信したい場合、データの複製に関しては注意を払う必要がある。特に、著作権を有するデータなどの配信に関し、データの複製を防止し、正確な課金処理をしたいという要望がある。

【０００３】

データの複製を防止するための一つの方法としては、データに暗号処理を施すという方法がある。例えば、データを配信するサーバ側で、送信するデータに暗号化処理を施し、データを受信するユーザ端末側でデータを復号化するような方法である。

【０００４】

しかし、文字情報や画像データなどのデジタルデータにおいては、たとえコンテンツ配信サーバ側が、送信するデータにコンテンツデータ複製防止のための暗号化処理を施したとしても、一旦ユーザ端末側でデータを復号化処理し、データ内容をディスプレイにより閲覧することが可能になると、そこからデータ複製が容易にできてしまうという問題点がある。

【０００５】

また、データの印刷を行う際にユーザ端末から印刷装置へ送信されるデータは暗号化されていないため、容易に複製ができてしまう問題点がある。これらは、デジタルデータの有料配信をしていく上での妨げとなっている。

【０００６】

【発明が解決しようとする課題】

本発明は、かかる問題点に鑑みてなされたものであり、ネットワークを介して、著作権を有するなど課金処理の必要な、あるいは、課金処理を望むデジタルコンテンツをユーザに対して配信するシステムに関して、第三者によるデータのデジタル複製を防止することを第１の目的としている。

【０００７】

また、ユーザに送信するデータに暗号化を施し、復号化機能を有する印刷装置内で復号化して印刷することにより、印刷して初めてコンテンツデータの内容を閲覧することのできる、暗号化印刷システムを提供することを第２の目的としている。

【０００８】

また、印刷装置に、データの暗号化および復号化に使用するための、装置固有の暗号鍵を与えておき、コンテンツ配信端末は、この暗号鍵をユーザ端末を介して取得し、この暗号鍵を用いて配信データに暗号化処理を施すことにより、別の印刷装置での印刷複製を防止する暗号化印刷システムを提供することを第３の目的としている。

【０００９】

また、印刷毎に上記の装置固有暗号鍵を変更するようにすることで、同一の印刷装置での複製も防止する暗号化印刷システムを提供することを第４の目的としている。

【００１０】

【課題を解決するための手段】

かかる目的を達成するために、請求項１記載の発明は、ネットワークを利用して、デジタルコンテンツのデータを配信する配信手段と、データを暗号化する暗号化手段とを有する配信端末と、配信端末からデータの配信を要求するユーザ端末と、ユーザ端末に接続され、暗号化手段により暗号化されたデータを復号化する復号化手段を有する印刷装置とを有し、配信端末は、ユーザ端末に要求されたデータを暗号化手段により暗号化してユーザ端末に送信し、ユーザ端末は、配信端末より受信したデータを印刷装置に送信し、印刷装置は、ユーザ端末より受信

したデータを復号化手段により復号化して印刷することを特徴としている。

【００１１】

請求項２記載の発明は、請求項１記載の発明において、配信端末は、ユーザに対しデータの配信に対する課金処理を行う課金処理手段をさらに有することを特徴としている。

【００１２】

請求項３記載の発明は、請求項１または２記載の発明において、印刷装置は、暗号化手段および復号化手段により使用される、印刷装置固有の、所定のデータ列から成る暗号鍵と、暗号鍵を管理し、ユーザ端末から暗号鍵の取得要求があった際、暗号鍵をユーザ端末へ送信する暗号鍵管理手段とをさらに有し、ユーザ端末は、あらかじめ、あるいは、配信端末より要求があった場合、印刷装置の暗号鍵管理手段より暗号鍵を取得して、配信端末へ送信し、配信端末は、ユーザ端末を介して取得した暗号鍵を用いて、暗号化手段により、ユーザ端末から要求されたデータを暗号化し、印刷装置は、ユーザ端末より受信した暗号化手段により暗号化されたデータを、暗号鍵を用いて、復号化手段により復号化することを特徴としている。

【００１３】

請求項４記載の発明は、請求項３記載の発明において、ネットワークは、インターネットであり、印刷装置は、ＩＰアドレスをさらに有し、暗号鍵はＩＰアドレスであることを特徴としている。

【００１４】

請求項５記載の発明は、請求項３記載の発明において、暗号鍵は、装置製造番号であることを特徴としている。

【００１５】

請求項６記載の発明は、請求項３から５のいずれか１項に記載の発明において、印刷装置は、ランダム変数を生成するランダム変数生成手段をさらに有し、暗号鍵管理手段は、ユーザ端末による暗号鍵の取得要求があった場合、ランダム変数生成手段によりランダム変数を生成し、暗号鍵に、ランダム変数を組み合わせて、ランダム暗号鍵を作成し、ランダム暗号鍵を保管およびユーザ端末へ送信し

、暗号化手段および復号化手段は、ランダム暗号鍵を使用してデータの暗号化および復号化を行うことを特徴としている。

【００１６】

請求項７記載の発明は、請求項６記載の発明において、ランダム変数生成手段は、ランダム変数として、現在時刻を利用することを特徴としている。

【００１７】

請求項８記載の発明は、請求項６記載の発明において、ランダム変数生成手段は、ランダム変数として、Ｔｏｔａｌカウンタの値を利用することを特徴としている。

【００１８】

請求項９記載の発明は、請求項１から８のいずれか１項に記載の発明において、印刷装置は、デジタル複写機能を有する複合機であることを特徴としている。

【００１９】

請求項１０記載の発明は、請求項１から８のいずれか１項に記載の発明において、印刷装置は、ファクシミリ機能を有する複合機であることを特徴としている。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。

【００２１】

図１は、本発明の第１の実施の形態におけるデータ配信システムの構成図である。

【００２２】

ユーザの端末１、サーバ２は、ネットワークを介して接続されている。印刷装置３は端末１とネットワークもしくは専用線などにより接続されており、データの送受を行うことができる。

【００２３】

ユーザ端末１は、サーバ２へアクセスするためのＷｅｂブラウザなどを備える。また、印刷装置３に対し印刷要求を行う。

【００２４】

サーバ２は、デジタルデータコンテンツを提供するＷｅｂサーバなどであり、提供するコンテンツの項目を表示する表示手段や、ユーザ端末１からのデータの選択や購入処理を受け付ける受け付け手段や、ユーザに対する課金処理手段などを有する。また、ユーザ端末１に送信するコンテンツデータを暗号化処理する暗号処理プログラムを有する。

【００２５】

印刷装置３は、サーバ２の有する暗号処理プログラムと同等の暗号処理プログラムを有する必要がある。印刷装置３は、ユーザ端末１を介して受信した被暗号化データを復号化処理してから印刷する。

【００２６】

まず、ユーザ端末１は、サーバ２へアクセスし、表示されるページから印刷を望むデータを選択する。サーバ２は、ユーザの選択したデータに暗号化処理を施して送信する。サーバ２からダウンロードされたデータは、複製を防ぐために、ユーザ端末１上では閲覧することはできない。ユーザは、ダウンロードした被暗号化データを印刷装置３に送信する。印刷装置３はユーザ端末１より受信した被暗号化データを復号化し、印刷を行う。ユーザは、印刷されたことで初めて要求したデータの内容を閲覧することが可能となる。

【００２７】

図２は、本発明の第２の実施の形態におけるシステムの構成図である。

【００２８】

第２の実施例では、印刷装置３は、あらかじめその印刷装置固有の暗号鍵を有する。暗号鍵は所定のデータ列から成る。この暗号鍵は、サーバ２における暗号化処理および印刷装置３における復号化処理において使用される。装置固有鍵として、装置の有するＩＰアドレスや製造番号を利用するなどの方法が考えられる。

【００２９】

サーバ２よりデータを購入する際、サーバ２は、データを暗号化するために使用する暗号鍵をユーザ端末１に対し要求する。ユーザ端末１は、印刷装置３から

暗号鍵を取得し、サーバ２に対しデータを要求すると共に、暗号鍵を送信する。サーバ２は、暗号鍵を受信し、この暗号鍵を使用してデータに暗号化処理を行い、暗号化されたデータをユーザ端末１に送信する。ユーザ端末１は、受信した被暗号化データを印刷装置３に送信する。印刷装置３は、受信したデータを暗号鍵に応じて復号化して印刷する。

【００３０】

図３は、本発明の第３の実施の形態におけるシステムの構成図である。

【００３１】

第３の実施例では、暗号鍵として、第２の実施例におけるような装置固有鍵に加え、さらにユーザ端末１からの暗号鍵の要求毎にランダムの変数を組み合わせて暗号鍵を作成する。

【００３２】

印刷装置１は、ランダム変数を生成する生成手段を有し、ユーザ端末１から暗号鍵の要求があった場合、ランダム変数を生成し、装置固有鍵と組み合わせて暗号鍵を作成し、ユーザ端末１へ送信する。以下同様に、この暗号鍵を用いて暗号化処理・復号化処理が行われる。また、ランダム変数として、印刷装置３の有する時計の現在時刻を用いたり、印刷装置３の有するＴｏｔａｌカウンタ（総プリント枚数を保持）の値を用いることが考えられる。

【００３３】

図４は、ランダム変数を用いた暗号鍵の仕組みを示す図である。

同一の印刷装置においても印刷毎に暗号鍵が変わるので、さらに複製がしづらいようになっている。

【００３４】

図５は、暗号処理の仕組みを示す図である。

別々の暗号鍵を用いて暗号化されたデータは、データとしては別のものである。また、ある暗号鍵を用いて暗号化されたデータは、同じ暗号鍵を用いないと復号化できない。本発明では、復号化処理を行うのは印刷装置３の内部ということもあり、第三者によるデータの複製が行われにくいのが特徴である。

【００３５】

図６は、第３の実施の形態におけるデータ配信システムの動作を示すフローチャートである。以下、図に沿って説明する。

【００３６】

ユーザは端末１からデジタルデータコンテンツを提供するサーバ２のＷｅｂページへアクセスする（ステップＳ１）。ユーザの端末１にはＷｅｂページが表示される（ステップＳ２）。ユーザは、ページの中から所望するデータを選択し購入の意思をサーバ２へ伝える（ステップＳ３）。

【００３７】

サーバ２はユーザ端末１に対し、データの暗号化処理のために使用する暗号鍵の要求をする（ステップＳ４）。ユーザは、その要求を受けて印刷装置３に対し暗号鍵を要求する。

【００３８】

印刷装置３は、ユーザ端末１からの要求を受けて、まずランダム変数を生成する。生成されたランダム変数と装置固有鍵を組み合わせて暗号鍵を作成する（ステップＳ６）。印刷装置３は、ユーザ端末１に暗号鍵を送信する（ステップＳ７）。生成したランダム変数あるいは暗号鍵は記憶しておき、データの復号化処理の際に使用される（ステップＳ８）。

【００３９】

ユーザ端末１は、サーバ２に暗号鍵を送信するとともにデータを要求する（ステップＳ９）。サーバ２は、被要求データを受信した暗号鍵に応じて暗号化処理し、ユーザ端末１に送信する（ステップＳ１０）。

【００４０】

ユーザ端末１は、サーバ２から被暗号化データを受信し（ステップＳ１１）、被暗号化データと印刷指示を印刷装置３へ送信する（ステップＳ１２）。

【００４１】

印刷装置３は、ユーザ端末１から被暗号化データと印刷指示を受信し、保存しておいた暗号鍵に応じて復号化する（ステップＳ１３）。そして復号化したデータは有効かどうかをチェックする（ステップＳ１４）。有効である場合（ステップＳ１４／ＹＥＳ）、データを印刷する（ステップＳ１５）。無効である場合（

ステップＳ１４／ＮＯ）、印刷は行わない。最後に印刷結果（完了／失敗など）をユーザ端末１へ送信し、終了する（ステップＳ１６）。

【００４２】

ユーザ端末１は、印刷装置３から印刷結果を受信し終了する（ステップＳ１７）。また、図には記載されていないが、データが無効であった場合などには、サーバ２へ通知する。

【００４３】

以上の処理を終了した後、サーバ２は、ユーザに対する課金処理を行い、終了する（ステップＳ１８）。

【００４４】

図７は、従来のデジタルデータ配信システムを示す図である。

インターネット上において、デジタルコンテンツのデータを提供するサーバ２とユーザの端末１がつながっている。ユーザは、端末１よりネットワークを介してサーバ２へアクセスし、所望するデータをダウンロードする。取得したデータは、自身の端末１上で自由に閲覧・編集することができる。また、印刷装置３で自由に印刷することができる。

【００４５】

図８は、図１のシステムの問題点を示す図である。

サーバ２からユーザ端末１へのデータ送信途中においては、データに暗号化処理を施すなどして複製を防止することができる。しかし、一旦ユーザがデータを取得すると、ユーザ端末１上およびユーザ端末１から印刷装置３へのデータ送信途中において複製が可能となってしまう。

【００４６】

【発明の効果】

以上の説明から明らかなように、請求項１記載の発明によれば、ユーザは暗号化されたデータを受信し、受信したデータを復号化機能を備えた印刷装置で印刷して初めてデータの内容を閲覧することができるようにすることにより、ユーザ端末上におけるコンテンツデータのデジタル複製を防止することができる。

【００４７】

請求項２記載の発明によれば、印刷して初めてコンテンツの内容を閲覧することができるシステムであるので、コンテンツデータに対する課金処理が行いやすくなる。

【００４８】

請求項３記載の発明によれば、印刷装置に装置固有の暗号鍵を与えておくことにより、ユーザ端末から印刷装置へ送信される印刷データを複製し別の同機能を有する印刷装置で印刷複製を得ることを防止することができる。

【００４９】

請求項４記載の発明によれば、装置固有鍵の設定を行わずに済む効果がある。

【００５０】

請求項５記載の発明によれば、請求項４記載の発明と同様に、装置固有鍵の設定を行わずに済む効果がある。また、ＩＰアドレスを有さない印刷装置であっても適用できる。

【００５１】

請求項６記載の発明によれば、暗号鍵を印刷毎に変更することにより、同一の印刷装置における印刷複製も防止することができる。

【００５２】

請求項７記載の発明によれば、請求項６記載の発明と同様に、暗号鍵を印刷毎に変更することにより、同一の印刷装置における印刷複製も防止することができる。

【００５３】

請求項８記載の発明によれば、請求項６記載の発明と同様に、暗号鍵を印刷毎に変更することにより、同一の印刷装置における印刷複製も防止することができる。

【００５４】

請求項９記載の発明によれば、デジタル複写機の機能を兼ねることができる。

【００５５】

請求項１０記載の発明によれば、ファクシミリ装置の機能を兼ねることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態におけるデータ配信システムの構成を示す図である。

【図２】

本発明の第２の実施の形態におけるデータ配信システムの構成を示す図である。

【図３】

本発明の第３の実施の形態におけるデータ配信システムの構成を示す図である。

【図４】

ランダム変数を用いた暗号鍵の仕組みを示す図である。

【図５】

暗号処理の仕組みを示す図である。

【図６】

本発明の第３の実施の形態におけるデータ配信システムの動作を示すフローチャートである。

【図７】

従来のデジタルデータ配信システムを示す図である。

【図８】

図１のシステムの問題点を示す図である。

【符号の説明】

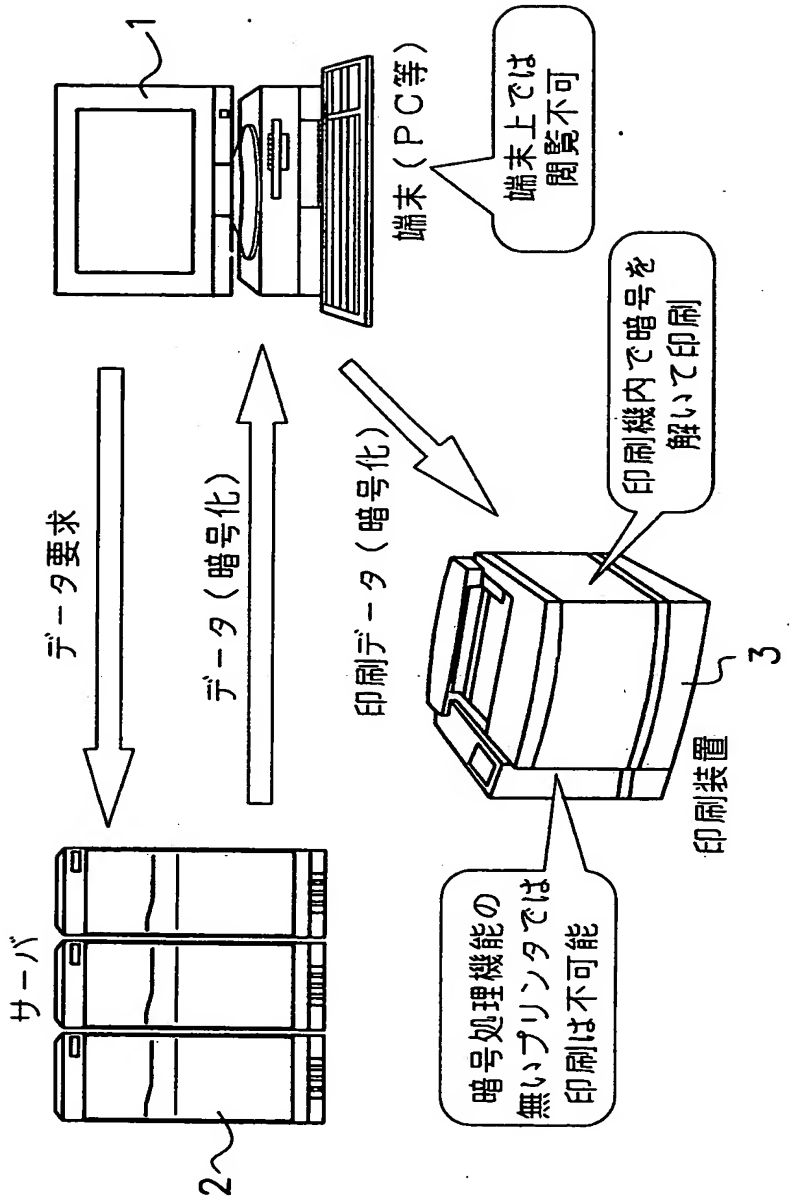
１　端末

２　サーバ

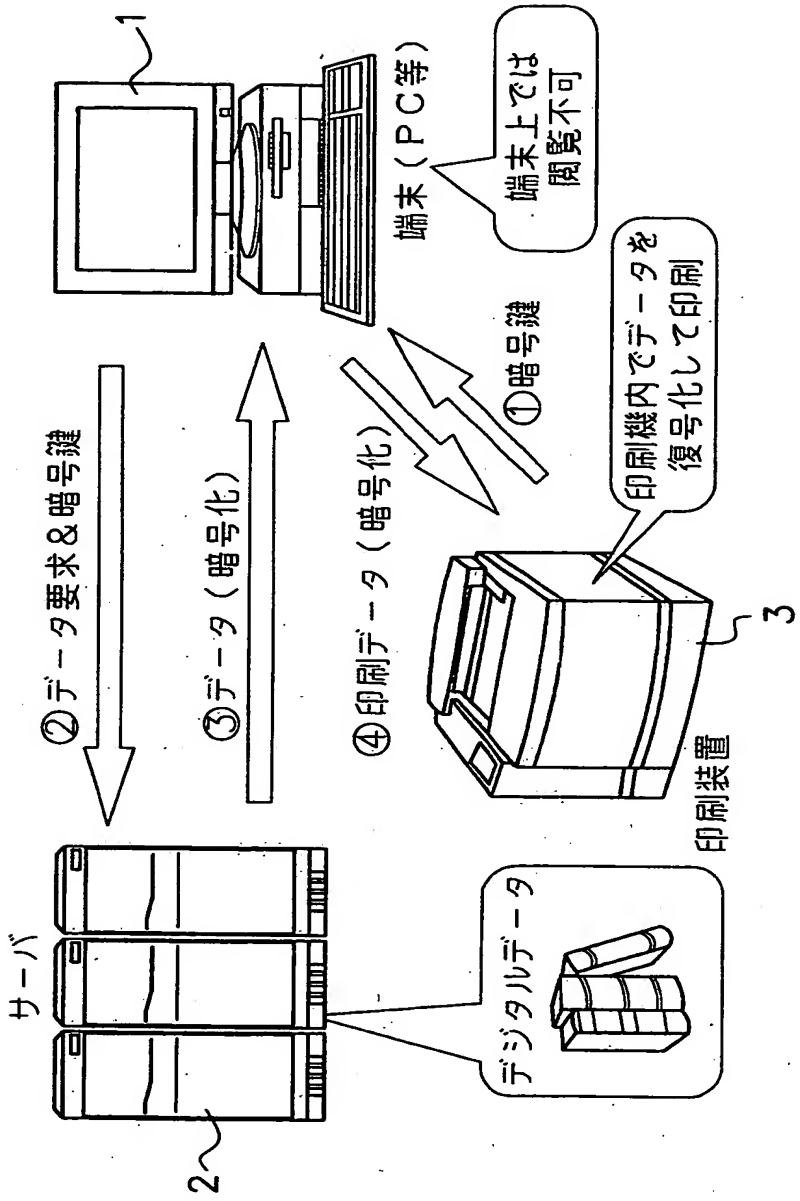
３　印刷装置

【書類名】　　図面

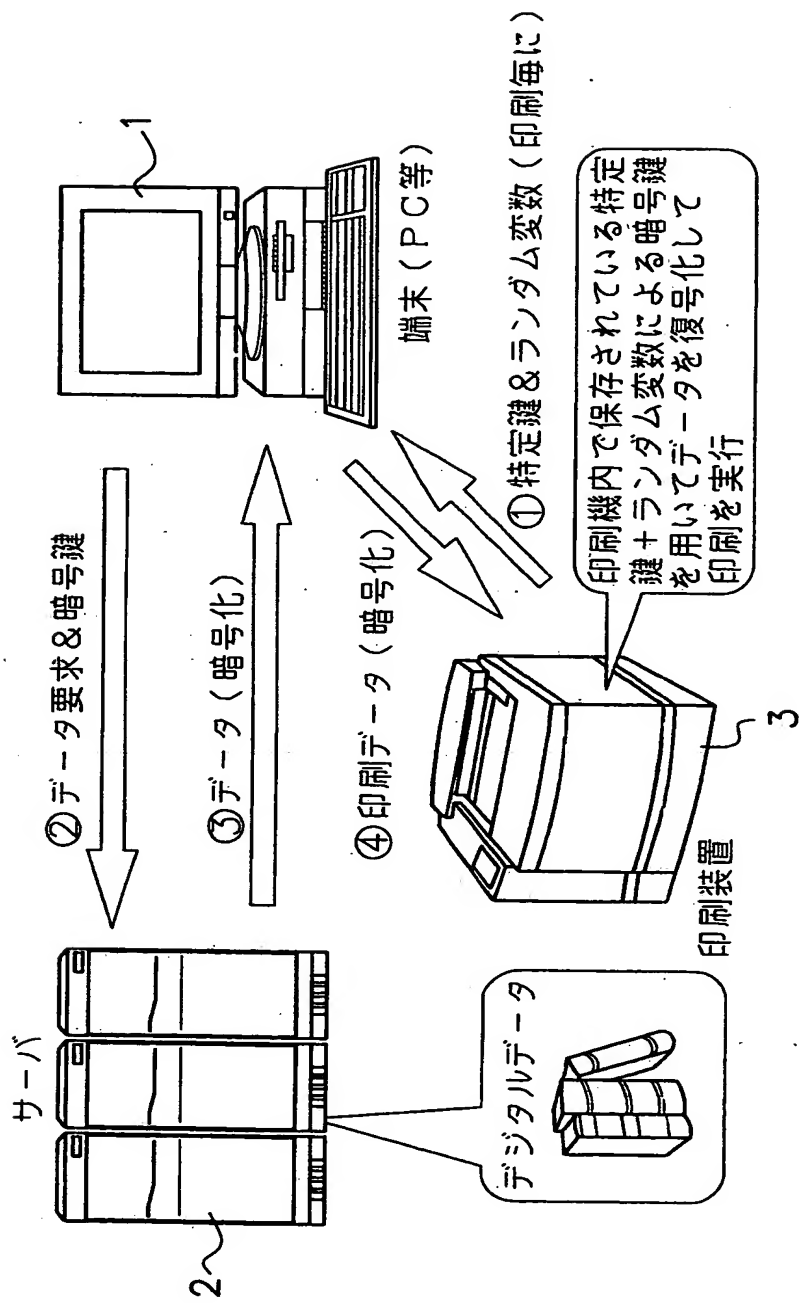
【図１】


1
端末（PC等）
端末上では
閲覧不可
データ要求
データ（暗号化）
印刷データ（暗号化）
印刷機内で暗号を
解いて印刷
3
印刷装置
サーバ
2
暗号処理機能の
無いプリンタでは
印刷は不可能

【図２】


1
端末（ＰＣ等）
端末上では
閲覧不可
①暗号鍵
②データ要求＆暗号鍵
③データ（暗号化）
④印刷データ（暗号化）
印刷機内でデータを
復号化して印刷
3
印刷装置
サーバ
デジタルデータ
2

【図３】


1
端末（ＰＣ等）
①特定鍵＆ランダム変数（印刷毎に）
印刷機内で保存されている特定鍵＋ランダム変数による暗号鍵を用いてデータを復号化して印刷を実行
②データ要求＆暗号鍵
③データ（暗号化）
④印刷データ（暗号化）
3
印刷装置
サーバ
デジタルデータ
2

【図４】

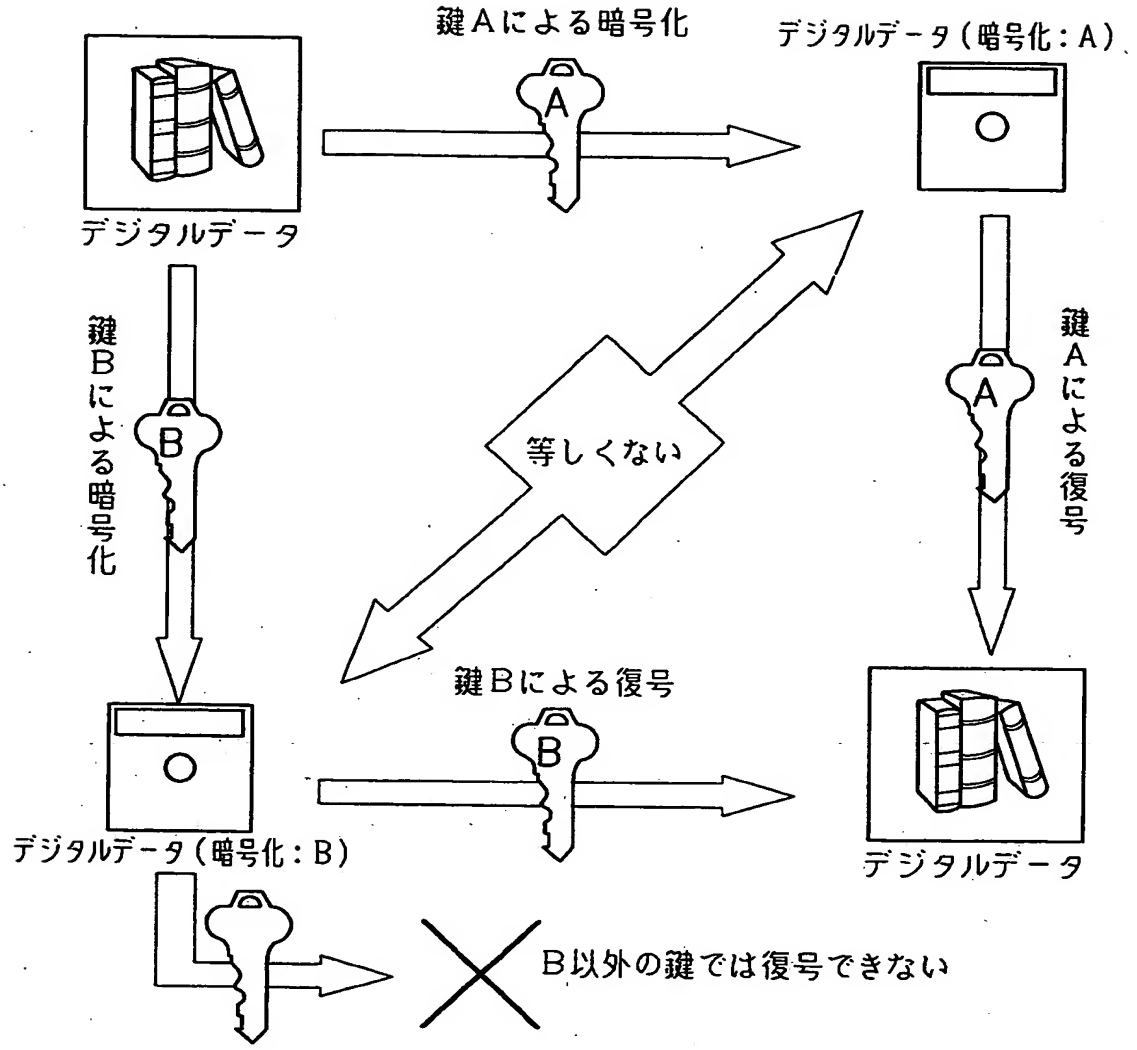
	マシン特定鍵		ランダム変数	暗号鍵	備考
１回目の印刷	AAAA	＋	BBB	EEEE	同一機器でも印刷毎に鍵が変わり、複製が出来ない様になる
２回目の印刷	AAAA	＋	CCC	FFFF	
Ｎ回目の印刷	AAAA	＋	DDD	GGGG	

注）AAAAはマシン固有

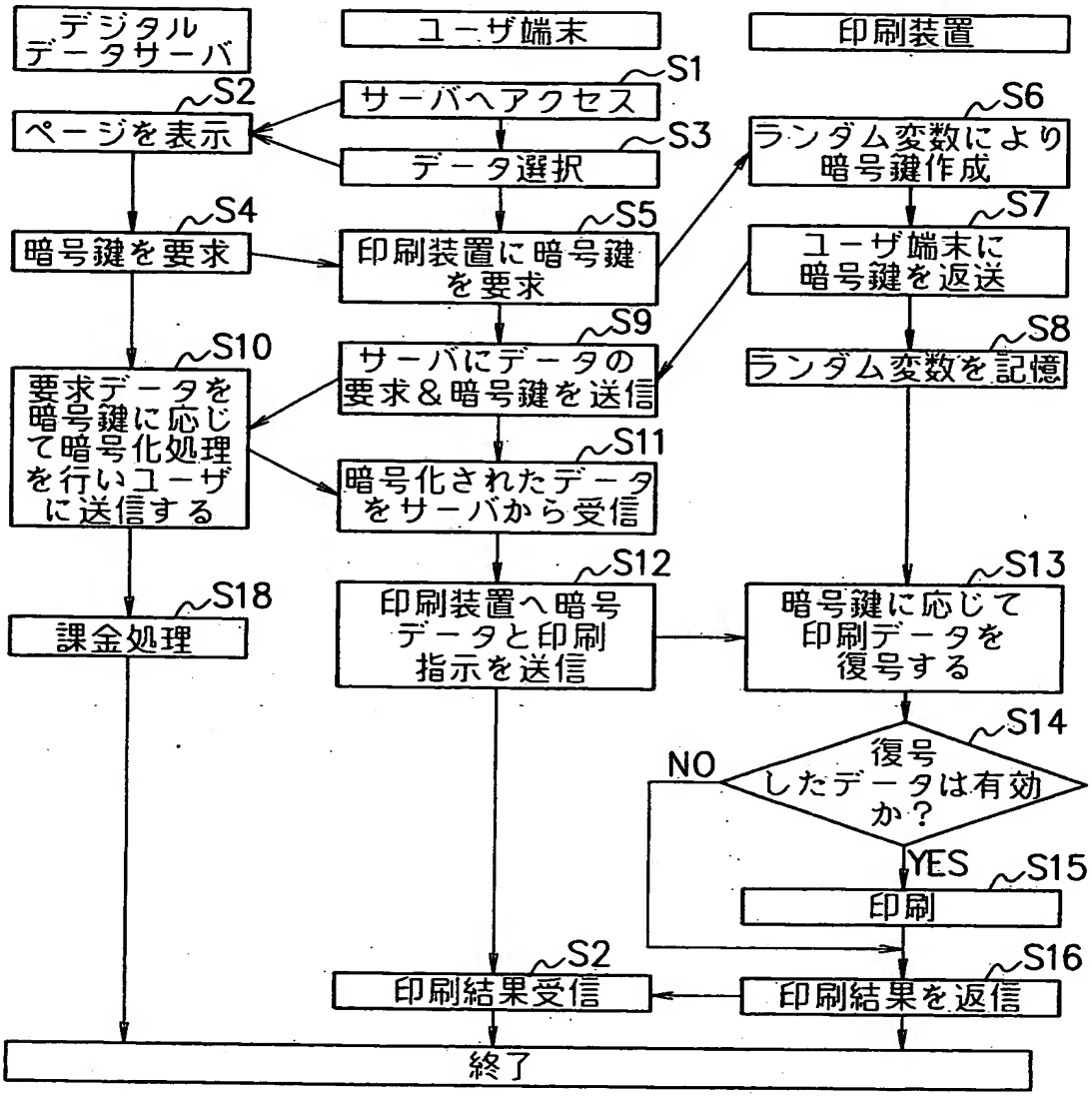
注）ＢＢＢからＤＤＤは、ランダム変数で印刷毎に印刷機で生成

注）ＥＥＥＥからＧＧＧＧは特定鍵とランダム変数を組み合わせた鍵

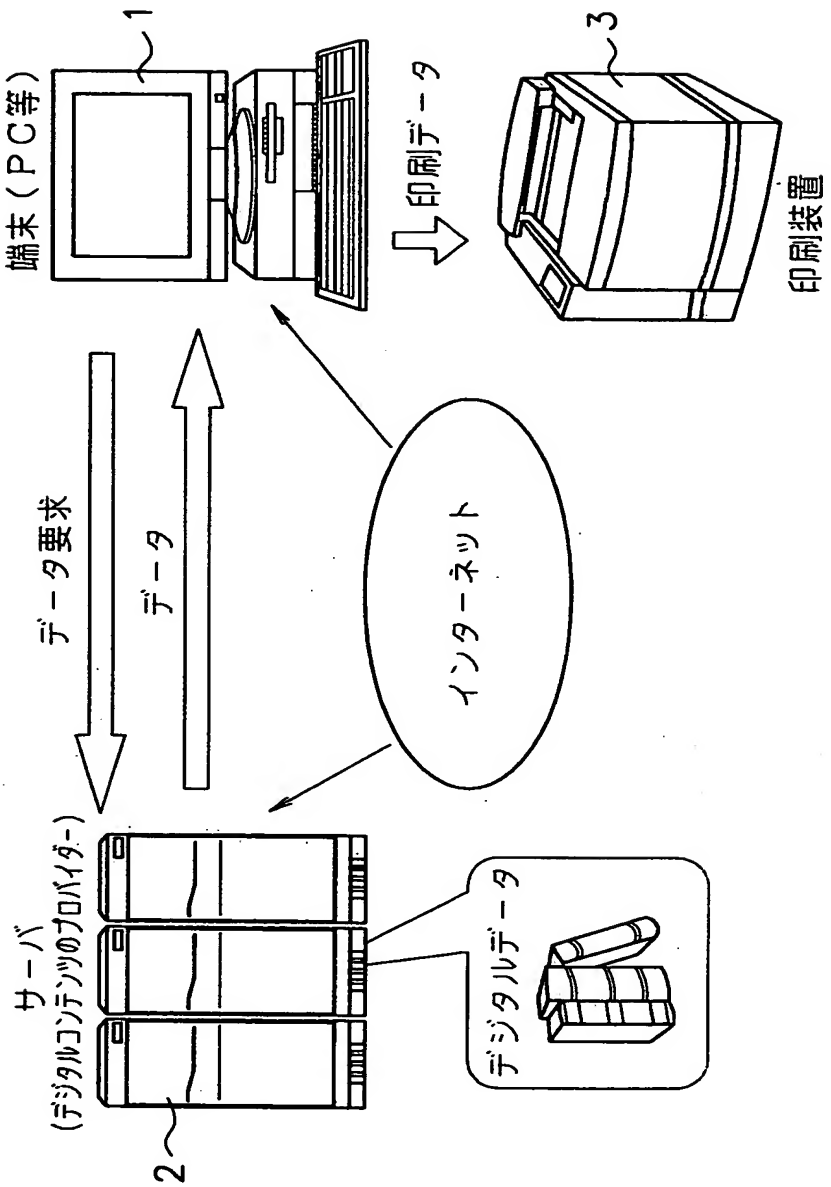
【図５】


鍵Ａによる暗号化
デジタルデータ（暗号化：Ａ）
デジタルデータ
鍵Ｂによる暗号化
鍵Ａによる復号
等しくない
鍵Ｂによる復号
デジタルデータ（暗号化：Ｂ）
デジタルデータ
Ｂ以外の鍵では復号できない

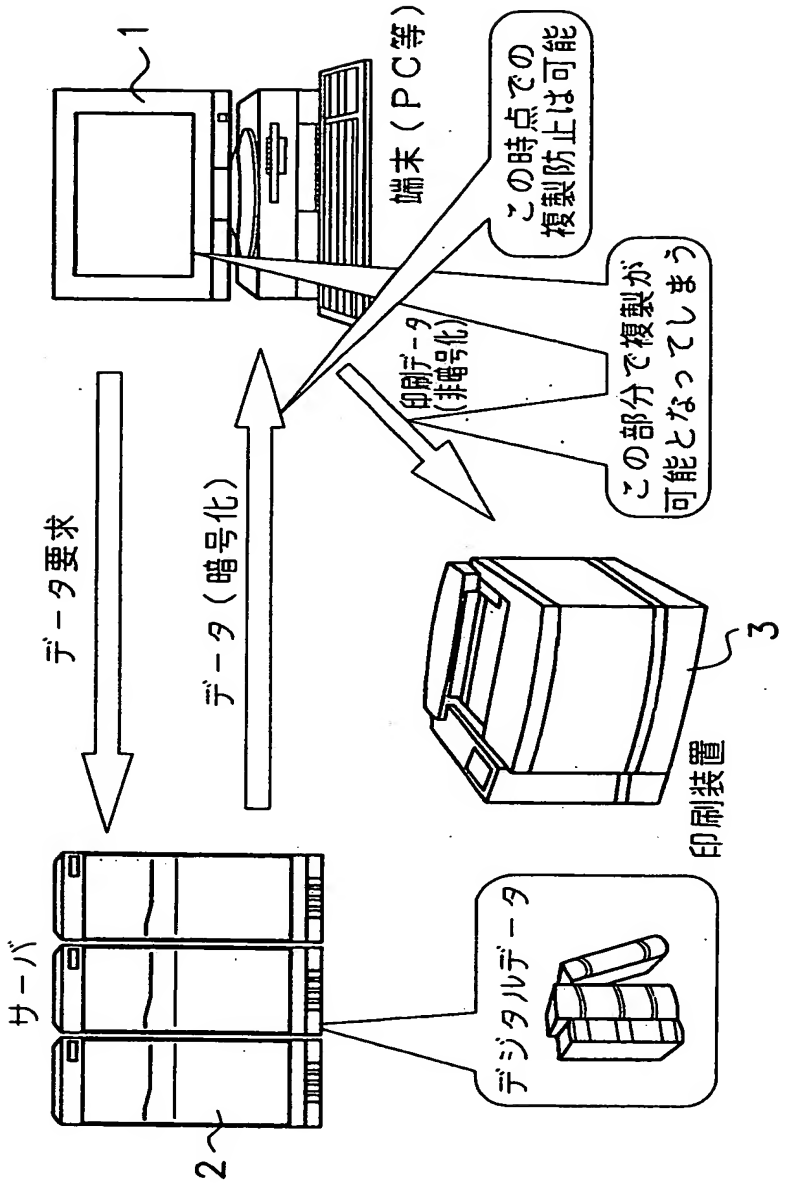
【図６】


デジタル
データサーバ
ユーザ端末
印刷装置
S1
サーバへアクセス
S2
ページを表示
S3
データ選択
S6
ランダム変数により
暗号鍵作成
S4
暗号鍵を要求
S5
印刷装置に暗号鍵
を要求
S7
ユーザ端末に
暗号鍵を返送
S9
サーバにデータの
要求＆暗号鍵を送信
S8
ランダム変数を記憶
S10
要求データを
暗号鍵に応じ
て暗号化処理
を行いユーザ
に送信する
S11
暗号化されたデータ
をサーバから受信
S12
印刷装置へ暗号
データと印刷
指示を送信
S13
暗号鍵に応じて
印刷データを
復号する
S18
課金処理
S14
復号
したデータは有効
か？
NO
YES
S15
印刷
S2
印刷結果受信
S16
印刷結果を返信
終了

【図７】


1
端末（PC等）
印刷データ
3
印刷装置
データ要求
データ
インターネット
サーバ
（デジタルコンテンツのプロバイダー）
デジタルデータ
2

【図８】


1
端末（PC等）
この時点での
複製防止は可能
印刷データ
（非暗号化）
この部分で複製が
可能となってしまう
データ要求
データ（暗号化）
3
印刷装置
サーバ
デジタルデータ
2

【書類名】　　要約書

【要約】

【課題】　ネットワークを介して、Ｗｅｂサーバなどによりデジタルコンテンツのデータをユーザの要求に応じて配信するシステムにおいて、データのデジタル複製や印刷複製を防止し、ユーザに対する課金処理を行いやすいシステムを提供する。

【解決手段】　ネットワークを利用して、デジタルコンテンツのデータを配信する配信端末は、データを暗号化する暗号化手段を備え、ユーザ端末よりコンテンツデータの配信を要求されると、データを暗号化して送信し、ユーザは、ユーザ端末において前記暗号化されたデータを受信し、受信したデータを、ユーザ端末に接続され、前記暗号化手段により暗号化されたデータを復号化する復号化手段を有する印刷装置へ送信し、印刷装置は、前記ユーザ端末より受信したデータを前記復号化手段により復号化して印刷することにより、ユーザは、所望するコンテンツデータを得る。

【選択図】　　図１

出願人履歴情報

識別番号　〔０００００６７４７〕

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー